

CLAIMS

We claim:

1. A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations.

2. The computer system of Claim 1, wherein said computer system further comprises a register file providing operands to said arithmetic logic unit.

3. The computer system of Claim 2, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey.

4. The computer system of Claim 3, wherein said datum is 64 bits long and said subkey is 48 bits long.

5. The computer system of Claim 3, wherein said first and second portions each contain one-half number of bits of said datum.

6. The computer system of Claim 5, wherein each of said first and second portions is 32 bits long.

7. The computer system of Claim 3, wherein said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first,

second and third registers to be operands in a subsequent execution of said instruction.

8. The computer system of Claim 7, wherein a
5 bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers.

10 9. The computer system of Claim 8, wherein said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit.

10. The computer system of Claim 1, further
15 comprising a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operating in parallel with said logic circuit.

11. The computer system of Claim 1, wherein said
20 logic circuit further comprises a circuit for selecting a subkey from a key.

12. The computer system of Claim 11, wherein said
25 key is 56 bits long.

13. A process for performing encryption or
decryption under a Data Encryption Standard (DES)
algorithm, comprising:

30 providing a logic circuit in an arithmetic logic unit; and
performing expansion permutation, S-box substitution and P-box permutation and associated XOR operations in said logic circuit.

14. The process of Claim 13, further comprising
35 performing shifting the output data of said logic circuit in a shift circuit in said arithmetic logic unit.

15. The process of Claim 14, further comprising:
storing operands in a register file; and
providing said operands to said logic circuit.

5 16. The process of Claim 15, further comprising:
storing a first portion of a datum for said
encryption or decryption in first register in said
register file;
10 storing a second portion of said datum for said
encryption or decryption in second register in said
register file; and
storing a subkey for said encryption or
decryption in third register in said register file.

15 17. The process of Claim 16, further comprising
storing operands of an instruction executing one round of
said DES algorithm in said first, second and third
registers using said logic circuit and said shift
20 circuit, said instruction designating to store results in
said first, second and third registers in such manner as
to allow said results in said first, second and third
registers to be operands in a subsequent execution of
said instruction.

25 18. The process of Claim 17, further comprising
providing said results as input to said logic circuit
without first being written back to said first, second
and third registers.

30 19. The process of Claim 13, further comprising
selecting a subkey from a key for said DES algorithm in a
second logic circuit.

35 20. The process of Claim 19, further comprising
operating said second logic circuit in parallel with said
logic circuit.

21. The process of Claim 13, further comprising selecting a subkey from a key using a key select circuit in said logic circuit.

00440224 00000000